# Dynamic security assessment by fuzzy inference

M.A. Matos
mmatos@inescn.pt

J.A. Peças Lopes
jpl@duque.inescn.pt

M. Helena Vasconcelos
mhv@bart.inescn.pt

Faculdade de Engenharia da Universidade do Porto (FEUP) and INESC-Porto, Portugal
Largo de Mompilher, 22, 4007 Porto Codex, Portugal

INESC-Porto, Portugal Largo de Mompilher, 22, 4007 Porto Codex, Portugal

**Abstract**
This paper reports an experience on the application of fuzzy reasoning to the fast assessment of the dynamic security of an isolated power system with high wind power penetration. The inference method is a Takagi-Sugeno type system with a small number of rules, optimized for each specific learning set by a standard method included in the MATLAB Fuzzy Logic Toolbox. The methodology is demonstrated in a contingency study in the network of Crete that showed good results in the test set. The paper discusses some implementation issues and possible future developments of the approach.

## 1. Introduction

Conventional dynamic security assessment of power systems is always a very time consuming analysis, unacceptable for real time applications. On the other hand, the foreseen increase of penetration of wind power in isolated systems can only be done if there is a fast way to evaluate security, due to the rapid changing conditions of the system, to the high possibility of sudden wind power losses and to the impact of short-circuit and similar situations.

These two facts lead to the development of a number of pattern recognition and machine learning approaches to this and similar problems of dynamic security assessment, namely k-Nearest Neighbor classifiers [1], Artificial Neural Networks [2], Decision Trees [3], Fuzzy Nearest Prototype classifiers [4] and Kernel Regression Trees [5]. A paper describing the application of the latter methodology to the network of Crete is presented in this Workshop [6]. The approach proposed in this paper belongs to same category of methods.

Note that the main issue is a classification problem: given a specific operating point (which is the *present* operating point) and some possible contingency (generator outage, sudden loss of wind power, short-circuit, etc.) we want to know, on-line, if the situation is secure or insecure, regarding the contingency. Of course, several contingencies must generally be considered in order to get a global evaluation of the present situation, which leads to the necessity of multiple studies like the one previously described.

Two approaches may be used regarding the classification problem: direct classification of the operating state, or inference of the value of some index or important variable, then used for classification. Some of the techniques can work with either philosophy. In the present case, frequency is a very important variable, and both $f_{min}$ and $df/dt_{max}$ values constitute usual security indices [6] that lead straightforward to decision rules based on thresholds to their values. In section XXX of this paper, the two approaches are used and results are compared.

In this paper, we are not going to describe the dynamic security assessment problem, or the way it is solved when execution time is not an issue. Those aspects can be seen in the companion paper [6], where the technical details of the generation of the learning and test sets are also addressed. We will only mention, in section XXXX, the necessary information needed to analyze the example.

Most of the paper is devoted to the analysis of the example and results, but a summary of the methodology and fuzzy inference systems is given in the next section. After the case study, the paper concludes with some indications of future developments and lines of work.

Preliminary

## 2. Methodology

As mentioned previously, the approach presented in the paper is based on the same general concept of the other pattern recognition or machine learning techniques, that is:

1. Generate a great number of operating points (OP), assuring diversity, randomness, etc.;
2. Divide randomly the OP in two sets (learning set, test set);
3. Use the Learning Set to train the classifier (or estimator), minimizing the training error;
4. Use the Test Set to check the generalization capability of the classifier (test error).

This is well-known [7], but some comments are necessary to fix terminology for the rest of the paper. In the first step, different operating situations are generated and analyzed regarding dynamic security, in a very time consuming simulation process. Each OP is therefore characterized by a number of attributes (variables usually available in the control center: p.ex. load, real and reactive generated power, spinning reserve, etc.), and by the indices or calculated variables that resulted from the simulation process (in this case, $f_{min}$, as mentioned earlier).

In the training process, selection of the relevant attributes can be made in different ways. We used a single ranking method based on the separability measure $F = \left|\mu_{\text{sec}} - \mu_{\text{insec}}\right| / \left(\sigma_{\text{sec}} + \sigma_{\text{insec}}\right)$, choosing the attributes with significant (greater) $F$, except when they are strongly correlated with variables previously chosen. The selected attributes are used as the input of the training process, while the corresponding value of $f_{min}$ (or the classification of the OP, if direct classification is wanted) is the output.

## 3. Fuzzy inference

The use of fuzzy sets as a powerful tool for describing qualitative or vague quantities lead to the definition of fuzzy *if-then* rules that could capture declarations about control processes , forecasting, estimation, classification, etc. For example:

**if** (load is high) **and** (reserve is low) **then** ($f_{min}$ is low)

In this rule, “high” and “low” are fuzzy qualifiers, that is, fuzzy sets defined in the universe of discourse of their respective variables (input: load, reserve and output: $f_{min}$). Figure 1 shows a possible set of qualifiers for reserve.

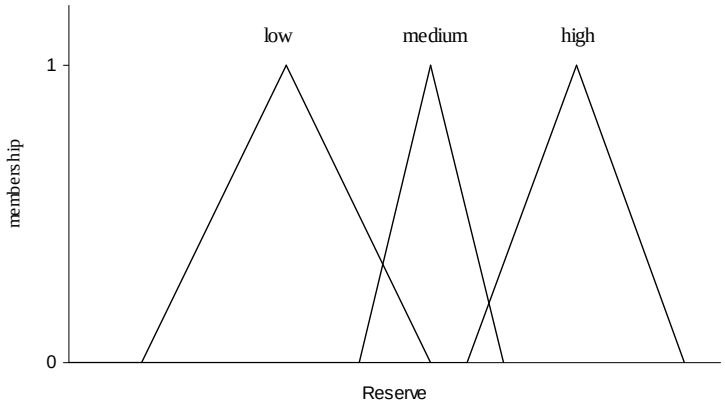


Figure 1 – Possible qualifiers for reserve

The contribution of each variable to the rule strength will be assessed using the corresponding membership function (fuzzification) and the operator "and" (in this case) will be applied next to determine the global degree of membership of the consequent (inference). For example, if the actual load is `0.7/high` and reserve is `0.5/low`, the rule will be fired with strength 0.35, assuming that we are using the product as "and" operator (a frequent alternative is the *min* operator).

The inference system will then consist on a set of rules that will be fired with different strengths, according to the inputs and the logical operators present in the rule. In order to generate the (crisp) result that is really the output of the system, it is necessary to combine the conclusions of all the rules (aggregation), and defuzzify (not necessarily by this order). The general scheme is shown is figure 2.

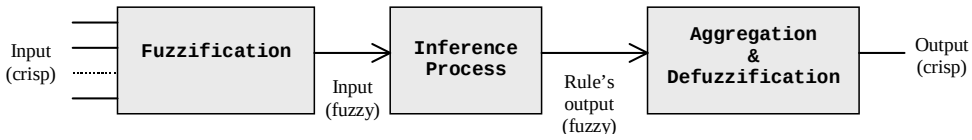


Figure 2 – General scheme of a fuzzy inference system

This general process may have variants, and can be implemented in many different ways [9], whose discussion is beyond the scope of this paper. We will now proceed to the particular type of system we used, the Takagi-Sugeno method [10].

The basic characteristic of the Takagi-Sugeno inference system is that the consequent of the rules is crisp, defined as a constant (zero-order system) or a linear combination of the input variables (first-order system). So, each rule has a crisp consequent with a degree of membership that comes from the antecedents, as for instance (first-order):

**if** (load is high) **and** (reserve is low) **then** ($f_{min}$=48+a*load+b*reserve)

were *a* and *b* are constants.

The output of the system is just the weighted average of all the consequents. Figure 3 (from MATLAB) depicts the set of 10 rules of study 3 (see section XXX), showing the influence of each input in each rule.

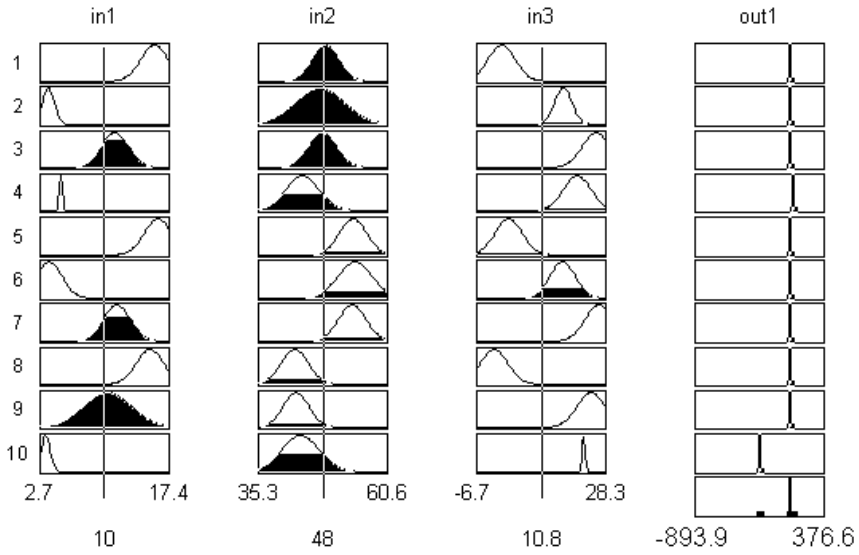


Figure 3 – Graphic description of rules for study 3 (input: 10, 48, 10.8)

The initial ideas about fuzzy inference systems [cimento] was to use rules that represent human knowledge and experience, captured by fuzzy descriptions of control variables. This conducts to interesting approaches in many situations, but a more efficient strategy uses a training process to define the rules and membership functions that minimize some error measure (vg the RMSE). Significance of the rules and membership functions is lost, but results are normally better than with "natural" approaches.

The process of training is based on backpropagation, and will not be described here. Details can be seen in [X] or directly in [jong 93], as we used the adaptive neuro-fuzzy system (ANFIS) included in the MATLAB toolbox for fuzzy logic.

Note that the Takagi-Sugeno (and other fuzzy inference systems) can be seen as a very flexible *nonlinear estimator*. To illustrate this feature, Figure 4 (from MATLAB) shows two surfaces that relate input variables to the output in study 3 (see section XXX).

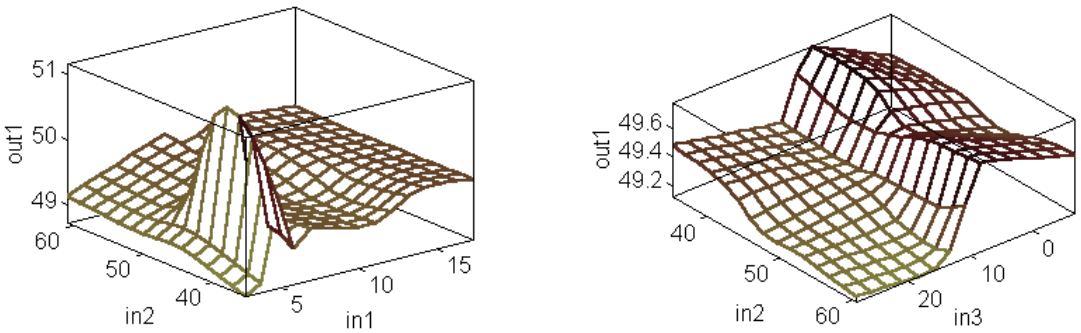


Figure 4 – Estimated $f_{min}$ as a function of pairs of input variables (study 3)

Finally, it is to point out that estimation of the output for a new OP is very fast, and therefore suitable for on-line purposes, even in very demanding situations.

## 4. Case study

The case study presented here is the same that was used in [6], and corresponds to the power system of Crete projected for the year 2000. It comprises several types of oil-fired units and a meshed 150 kV transmission network. The conventional generation system consists of two major power plants with twenty generating units installed. A total of 11 Wind Parks (WPs) consisting of 160 Wind Turbines (WTs) with an installed capacity of more than 80 MW are or will be installed by the year 2000. However, the data set exploited in this paper corresponds to a machine loss disturbance, which is not the disturbance considered in paper [6].

As a result, in case of faults on some particular lines the majority of the wind parks will be disconnected. Furthermore, the protections of the WTs might be activated in case of frequency variations, decreasing additionally the dynamic stability of the system. This might be caused by wind fluctuations, conventional unit outages, faults or other disturbing conditions.

In the reported experiences, we used a zero-order system.

### 4.1. Attribute selection and learning set generation

Each operating point was characterized by a set of initial attributes, which included, active powers produced by wind parks, active power produced by conventional units, their spinning reserve, wind penetration, wind margin, total active and reactive loads and reactive generation in capacitor banks.

For the Crete case study, the generation of the data set was developed by National Technical University of Athens (NTUA), within the framework of the CARE project. A short description of the way how this was obtained can be found in [6].

After applying the *F* measure, attributes 14, 10, 5 and 4 were selected as the most relevant, because they have the best values of *F* and not correlated to each other (most of the other original attributes are). These attributes correspond respectively to the spinning reserves in power plants 4 and 2, total active power produced by the wind parks and active power produced by wind park number 4.

The F values were obtained assuming that the operating points of the learning set were separated according to the following decision rule:

```
if fmin>49 Hz then system is secure else system is insecure
```

With this hard classification the operating points available in the data set were splited in two classes (secure/insecure) as described in Table 1.

Table 1 – Generated operating points

| | **Learning set** | **Test set** |
|---|---|---|
| Secure OP | 31 | 20 |
| Insecure OP | 1813 | 901 |
| **Total** | **1844** | **921** |

To ease the interpretation of the results and figures, the OP are ordered from the least to the greater value of $f_{min}$.

### 4.2. First study: direct classification

In the first study, the original learning set was used, with the binary output resulting from the application of the classification rule. After 100 epochs of training, a minimum RMSE of 0.0537 was obtained, as shown in figure 5.

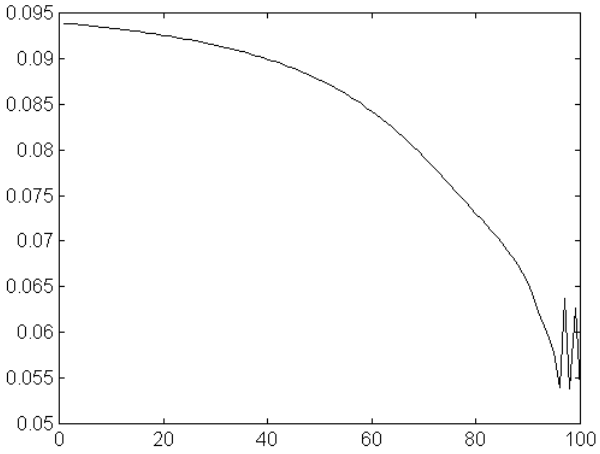


Figure 5 – Study 1: RMSE evolution during the training phase (100 epochs)

Because we are seeking for a classifier, training and test errors are more meaningful in terms of false and missed alarms, as reported in table 2.

Table 2 – Classification results (study 1)

| | **Training** | | **Testing** | |
|---|---|---|---|---|
| Missed alarms | 3 | 9.7% | 7 | 35% |
| False alarms | 0 | 0 | 0 | 0 |
| **Total** | **3** | **0.16%** | **7** | **0.76%** |

Although the global results are good, the missed alarms error is rather excessive, apparently due to the fact that the number of insecure points in the Learning set (31) is excessively small.

### 4.3. Second study: direct classification (modified learning set)

Trying to cope with the difficulty identified in the first study, we increased artificially the number of insecure points in the learning set, by considering each one of them three times in a modified learning set. So, the number of insecure OP increased to 93, and the total number of points changed to 1906). The corresponding results are described in table 3:

Table 3 – Classification results (study 2)

| | **Training** | | **Testing** | |
|---|---|---|---|---|
| Missed alarms | 0 | 0 | 4 | 20% |
| False alarms | 1 | 0.06% | 0 | 0 |
| **Total** | **1** | **0.05%** | **4** | **0.43%** |

These results, still not satisfactory regarding the missed alarms error, were obtained after 100 epochs, with a RMSE of 0.0736. A second take with 500 epochs originated a smaller RMSE of 0.0552, but the classification performance didn't improve.

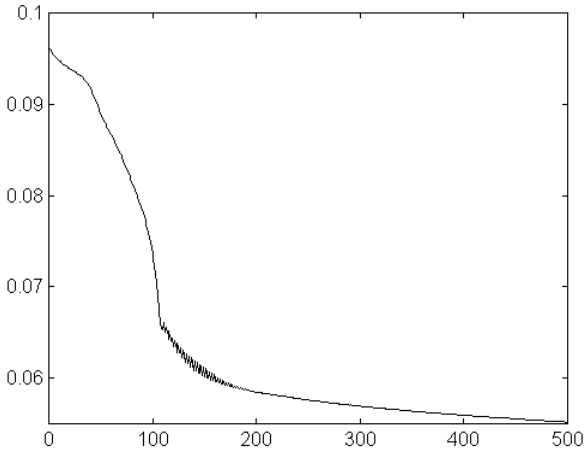


Figure 6 – Study 2: RMSE evolution during the training phase (500 epochs)

Figure 7 shows the results (first 80 OP) from the inference process in this study, were an output greater than 0.5 was classified as secure, while a value less than 0.5 lead to the insecure class. Reference classifications obviously take only the values 0 (insecure) or 1 (secure).

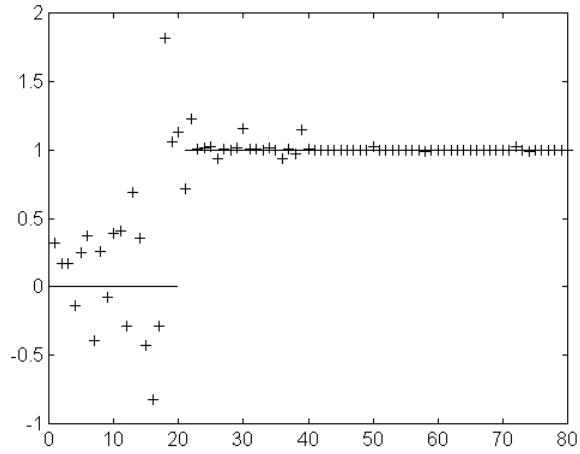


Figure 7 – Study 2: Correct (-) and estimated (+) values of the classification on the Test set (detail)

### 4.4. Third study: $f_{min}$ estimation (modified learning set)

To design a fuzzy inference system to estimate the value of $f_{min}$, we used the inputs of the modified learning set (as in study 2) with the corresponding values of $f_{min}$ obtained in the original analysis, as mentioned in section 4.1.

A number of experiments was performed with different parameters' instances for the optimization algorithm. Figure 8 shows the evolution of the RMSE (until 0.0775) for 1000 epochs training in the selected configuration, but best results were obtained when the process stopped at 250 epochs, although the RMSE is worse (0.0928).

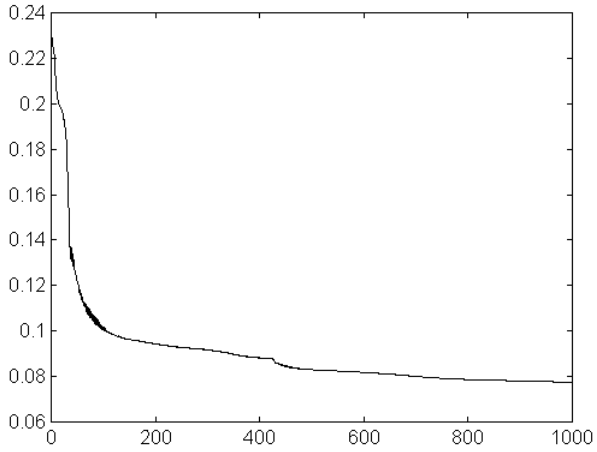


Figure 8 – Study 3: RMSE evolution during the training phase (1000 epochs)

This is due to overfitting to the secure points of the learning set, that leads to the increase of missed alarms, both in the learning and test sets. Table 4 shows the results, again in terms of classification with the same decision rule mentioned in section 4.1.

Table 4 – Classification results (study 3)

| | **Training** | | **Testing** | |
|---|---|---|---|---|
| Missed alarms | 0 | 0 | 2 | 10% |
| False alarms | 5 | 0.28% | 2 | 0.22% |
| **Total** | **5** | **0.27%** | **4** | **0.43%** |

Comparison of correct and estimated values of $f_{min}$ for the first 100 OP of the test set is shown in figure 9.

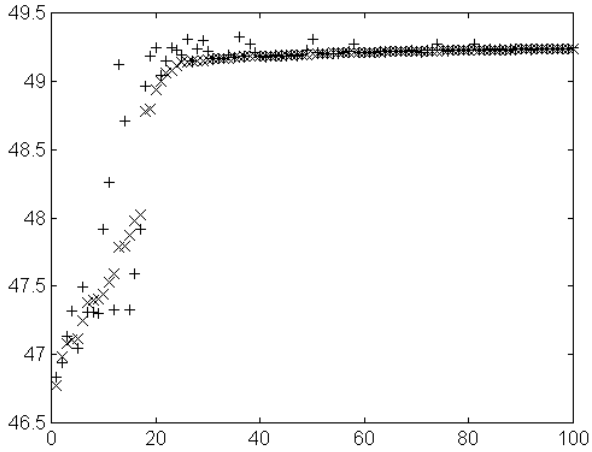


Figure 9 – Study 3: Correct (x) and estimated (+) values of the classification on the Test set (detail)

## 5. Conclusions

Results of the application of fuzzy inference systems to dynamic security assessment are very promising, even when only a general purpose package was used to design the system.

However, more extensive tests are certainly needed, with different learning sets and contingency situations, in order to draw more definite conclusions.

Future development of this work include the use of different types of fuzzy inference systems (first-order Takagi-Sugeno, different logical operators, etc.), new training algorithms and new training philosophies, namely for the direct classification procedures, with minimization of the classification error instead of the RMSE.

## 6. References


[1] Peças Lopes, J. A., Maciel Barbosa, F. P. and Marques de Sá, J. P., "On-line transient stability assessment and enhancement by pattern recognition techniques", Electric Machines and Power Systems Journal, vol.15, 1988.

[2] Sobajic, D.J., and Pao, Y.H., "Artificial neural-net based security assessment for electric power systems", IEEE Trans. on PWRS, Vol. 4, nr. 1, February 1989.

[3] Hatziargyriou, N., Peças Lopes, J. A.,, Papathanassiou, S., Van Acker, V., Fidalgo, J. N., "Dynamic security assessment using pattern recognition, neural networks and decision trees - Results in the Lemnos Power System", JOU2-CT92-0053 internal progress report, November 1993.

[4] Manuel Matos, N. Hatziargyriou and J. A. Peças Lopes, "Fuzzy Steady State Security Assessment", Proc. Sotckholm Power Tech., Sotckholm, June 1995.

[5] J. A. Peças Lopes, Fernando Fernandes, "Fast evaluation of Voltage Collapse Risk Using Machine Learning Techniques", Invited paper presented to the VI SEPOPE, S. Salvador da Baia, May 1998

[6] M. H. Vasconcelos, J. A. Peças Lopes, "Pruning Kernel Regression Trees for security assessment of the Crete Network", To be presented at the ACAI workshop, Crete July 1999.

[7]
[8]
[9]



**Acknowledgments**: The authors would like to thank the financial support of PRAXIS XXI within the "Subprograma Ciência e Tecnologia do 2º Quadro Comunitário the Apoio" and to EU project JOR3-CT96-0119. They are also grateful to all the other members of the project JOR3-CT96-0119 for their contributions, specially to Prof. Hatziargyriou for the learning set data of the Crete network used in this paper.